



DII COE IAVA Implementation Process

~~May 2001 CRCB~~

**Matt O'Brien
obrienma@saic.c
om**

**Quang Nguyen
nguye2q@ncr.disa.mil
DII COE Security Engineer**

9 May 2001



Outline

- **CRCB Actions Being Addressed**
- **DII COE Information Assurance Vulnerability Alert (IAVA) Implementation Process Flow Diagram**
- **Benefits of COE IAVA Implementation Process**
- **DII COE IAVA Review Team Process**
- **Vulnerability Sources**
- **Vulnerability Ratings**
- **Current Risk Management Strategy**
- **Proposed Risk Management Strategy**
- **Decisions Requested Today**

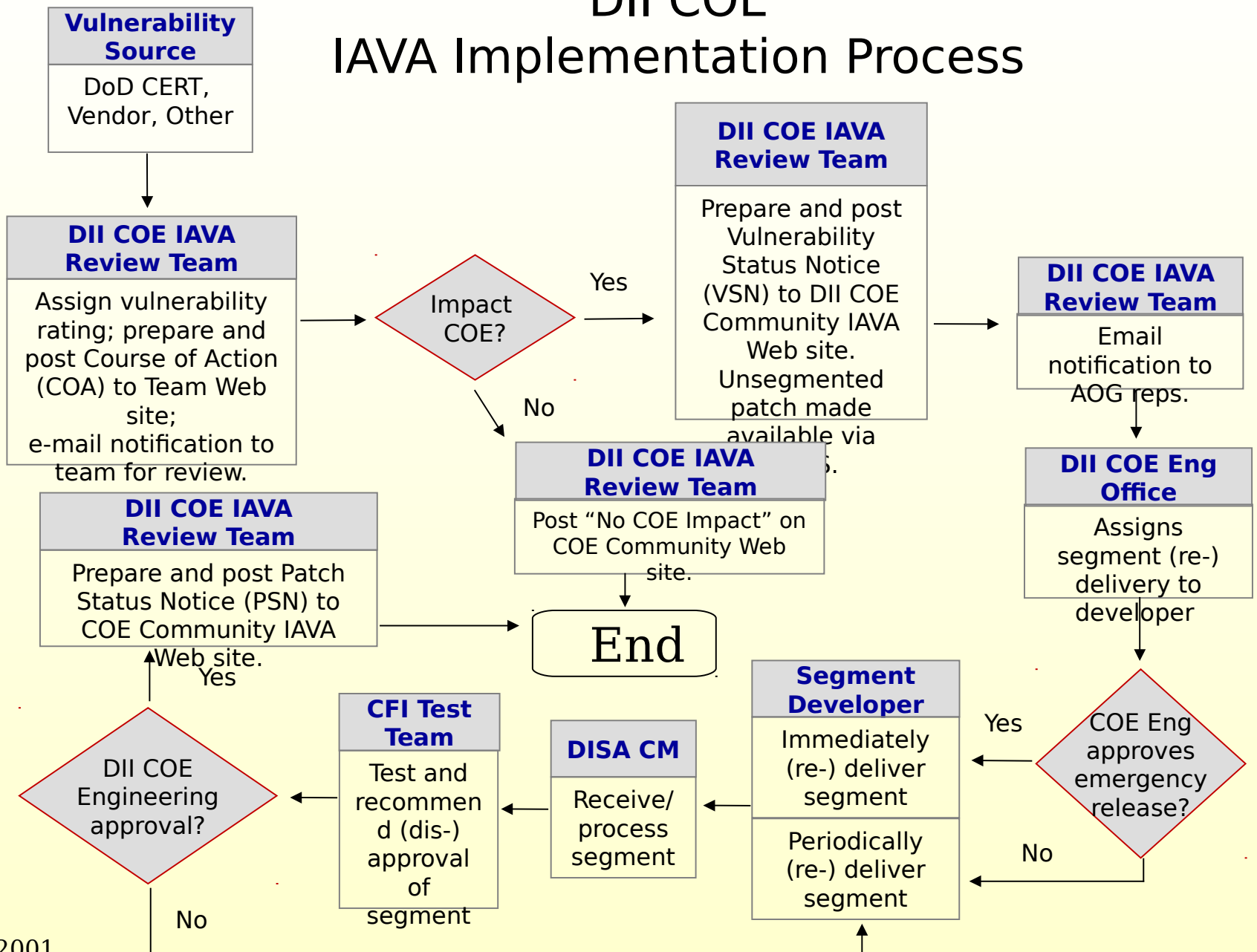


CRCB Actions Being Addressed

- **01-001 - AOG to develop risk management criteria for removing JREs and provide recommendations to the CRCB**
- **01-002 - COE to work with Joint Staff (J6-K) to coordinate the JRE risk management strategy**
- **01-003 - COE to provide white paper on end-to-end COE IAVA management process**

DII COE

IAVA Implementation Process





Benefits of COE IAVA Implementation Process

- **Process identifies vulnerabilities specific to COE baseline that are not addressed by DoD IAVA process**
- **Process provides an analysis and triage function for vulnerabilities applicable to all COE-based systems**
- **Patch testing process ensures the Hippocratic Oath is observed: “First Do No Harm”**



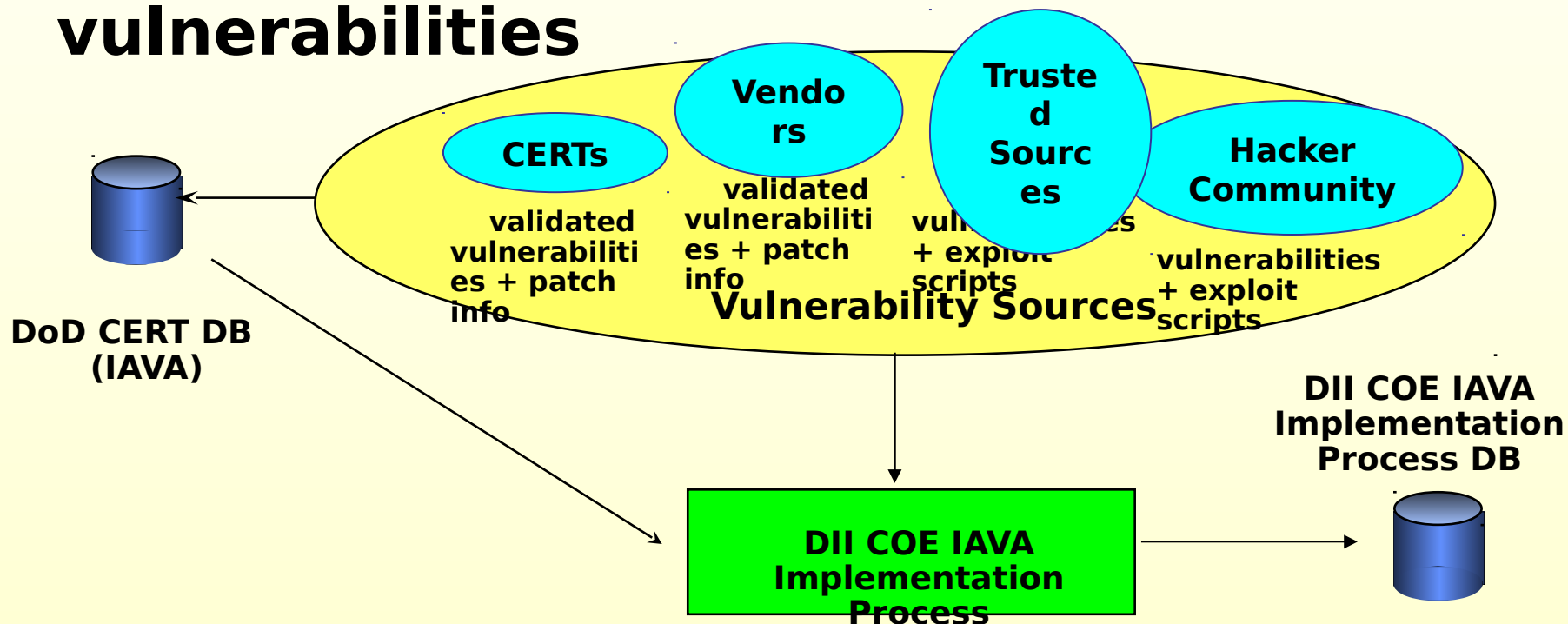
IAVA Review Team Process

- **Contractor support provides research and analysis for vulnerabilities, and assigns vulnerability ratings for non-IAVA vulnerabilities**
- **E-mail notification to IAVA Review Team that a Course of Action (COA) report has been posted to IAVA Review Team Web site**
- **IAVA Review Team reviews and endorses COA**
 - **DISA has final decision-making authority**
- **Contractor support posts Vulnerability Status Notice to DII COE Community IAVA Web site & e-mails AOG reps.**
- **Contractor support posts Patch Status Notice when segmented patch has been released**



Vulnerability Sources

- **DII COE IAVA Implementation Process tracks both IAVA and non-IAVA vulnerabilities**





Vulnerability Ratings

- **A vulnerability rating is assigned to each DoD IAVA and COE IAVA (internally generated)**
- **DoD CERT assigns DoD IAVA ratings; COE assigns COE IAVA ratings**
- **Vulnerability ratings provide a triage function, describing the operational impact of the vulnerability and required response times**
- **The following ratings and response times are used:**

Critical

24 hours

Priority

3 business days



Vulnerability Ratings (2)

- **Vulnerability ratings definitions are based upon MIL STD 498 (now IEEE Std 1044)**

- **Critical (Priority 1)**

Vulnerability poses a serious threat to DoD systems/infrastructures.

Criteria:

Exploit is executable from a remote location.

Exploit has significant impact (e.g., denial of service, root compromise).

Exploit affects a large number of installed hosts in their standard configuration or infrastructure systems.

Exploit code is available and currently being used to exploit systems.

- **Priority (Priority 2)**

Vulnerability poses a serious threat to DoD systems.

Criteria:

Exploit has significant impact (e.g., denial of service, root compromise).

Exploit affects a large number of installed hosts in their standard configuration or infrastructure systems.

- **Routine (Priority 3)**

Vulnerability poses a threat to DoD systems.

Criteria:

Exploit affects a large number of hosts in their standard configuration or the underlying infrastructure.

Exploit adversely affects the accomplishment of an essential capability (e.g.,



Current Risk Management Strategy

- **Critical**
 - **Fix to be provided via emergency security patch segment release**
- **Priority**
 - **Fix to be provided on schedule directed by the COE Chief Engineer**
- **Routine**
 - **Fix to be provided in scheduled patch update or COE release**



Proposed Risk Management Strategy

- **Upon discovery of a CRITICAL or PRIORITY vulnerability for which no patch or workaround is expected:**
 - **COE office will notify AOG that the vulnerable software version will be removed from the COE repository**
 - **Replaced with a new, secure version (if possible)**
 - **If removal will result in significant cost impact to the COE, CRCB will be consulted**
 - **System PMs will decide whether or not to continue using the vulnerable software version to support current operations**



Decisions Requested Today

- **01-001 - AOG to develop risk management criteria for removing JREs and provide recommendations to the CRCB**
 - Recommend that CRCB accept proposed risk management strategy and close action
- **01-002 - COE to work with Joint Staff (J6-K) to coordinate the JRE risk management strategy**
 - Will remain open until MOU established between DISA and JS regarding proposed risk management strategy
- **01-003 - COE to provide white paper on end-to-end COE IAVA management process**
 - Recommend closure: white paper delivered today and explained via this briefing



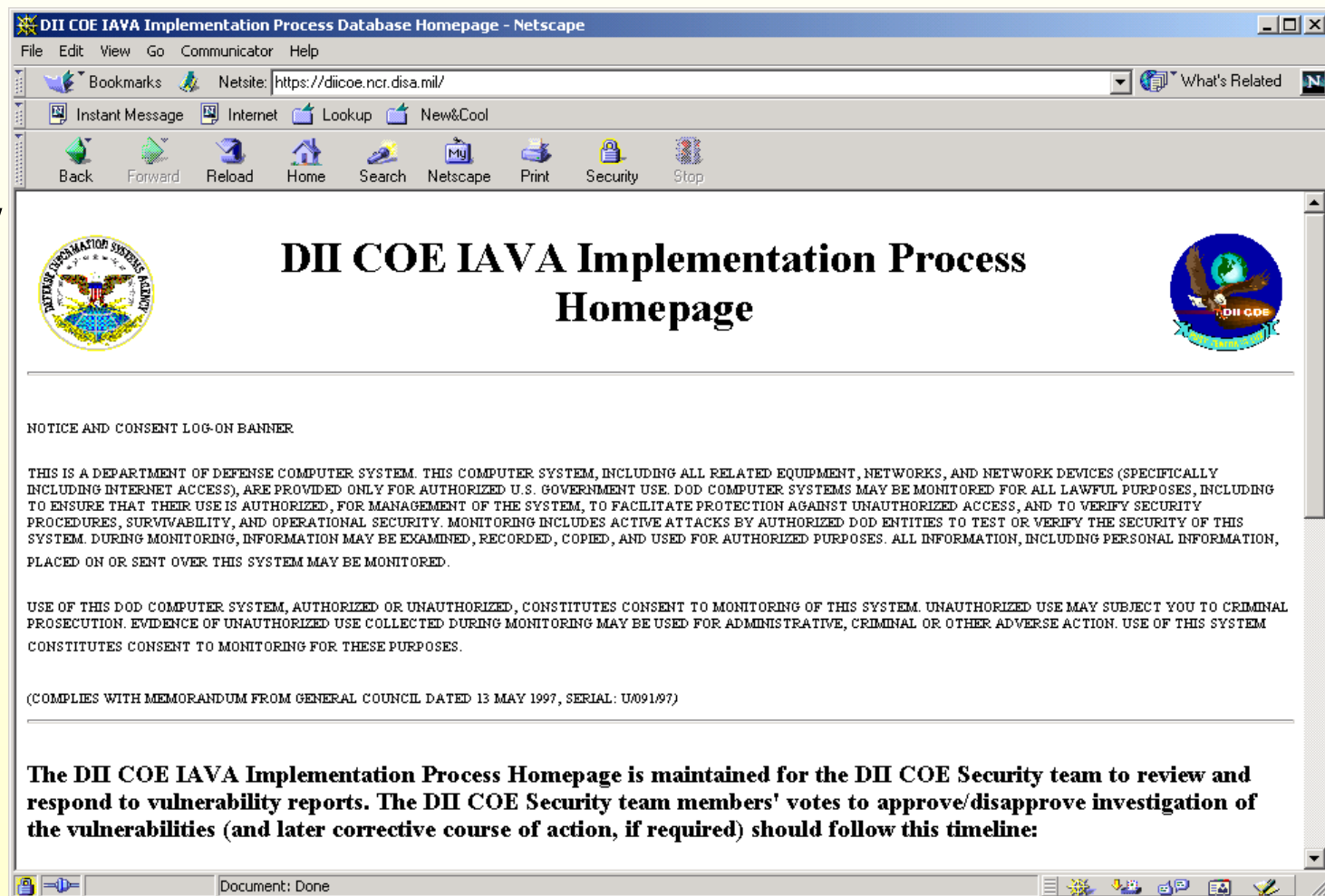
Back-up Slides



DII COE JAVA Review Team Web Site

Username/
password
protected

Secure
Sockets
Layer





Course of Action

Courses of Action - Netscape

File Edit View Go Communicator Help

Bookmarks Netsite: <https://diicoe.ncr.disa.mil/reports/coe01-012B-COA.html> What's Related

Instant Message Internet Lookup New&Cool

Back Forward Reload Home Search Netscape Print Security Stop

DII COE Vulnerability COA Recommendation Report

This report provides the results of an assessment on the impact of the referenced vulnerability on the DII COE and provides a recommended Course of Action (COA). This vulnerability has been identified as **Routine**.

Request that you review and/or approve the impact assessment and COA recommendation and forward your response within 5 days by replying to the email notification alerting you to this report.

This DII COE Vulnerability COA Recommendation Report will be followed by update reports, if required, and by a Security Patch Notice when a security patch has been developed.

Course of Action Number: COE01-012B-COA

Date: 02/12/2001

Update Date: 02/13/2001

Rationale:

There is a third notification from DoD.CERT to this virus:

- 1) The threat level is now "MEDIUM".

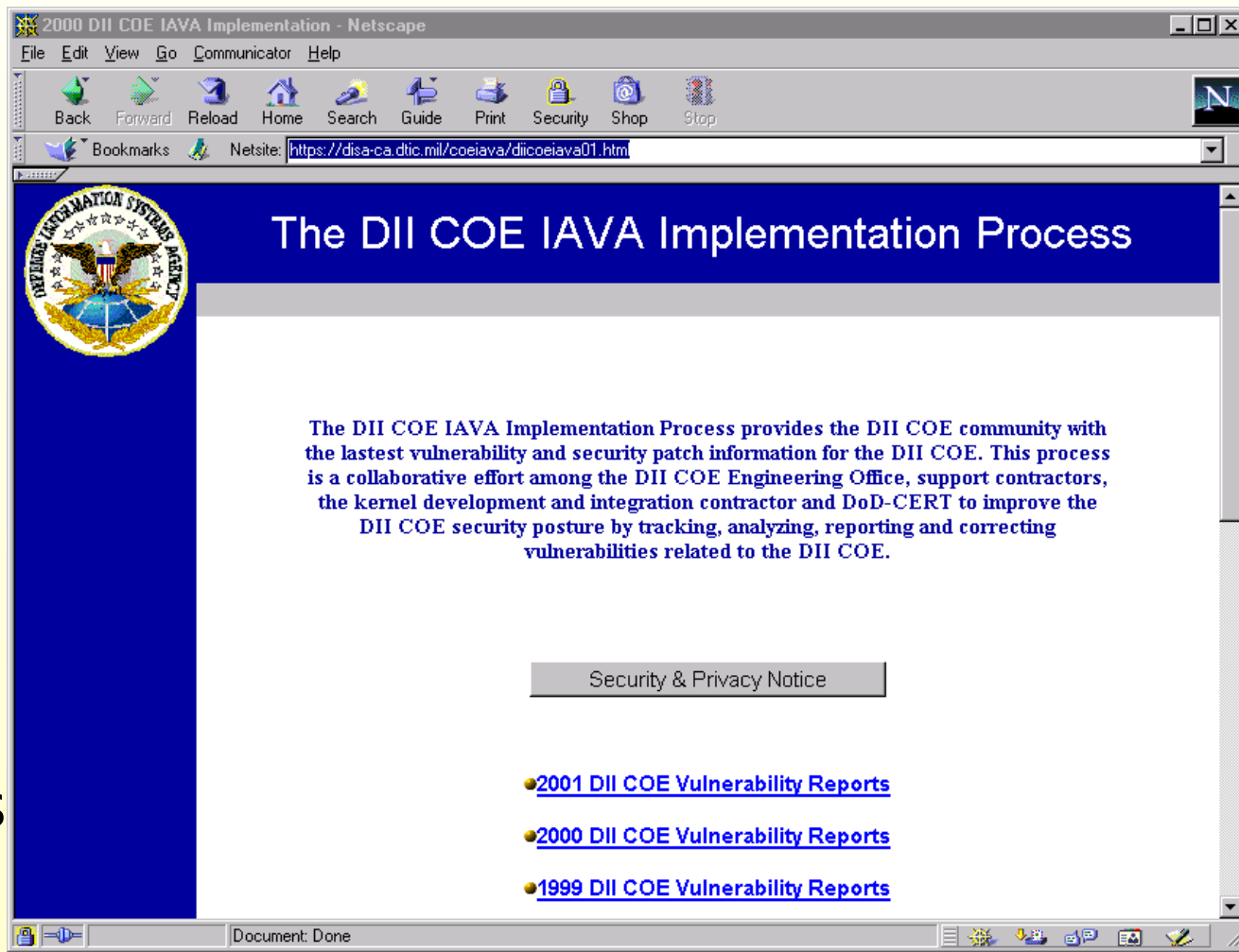




DII COE Community JAVA Web Site

Secure
Sockets
Layer

Restricted
to
*.mil
IP
Addresses



5/9/2001

<https://disa-ca.dtic.mil/coeiava/diicoeiava01.html>



2001 Vulnerabilities

2001 DII COE IAVA Implementation - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Guide Print Security Shop Stop

Netsite: <https://disa-ca.dtic.mil/coejava/diicoejava01.htm>

2001 DII COE IAVA Implementation Process

This table contains BOTH the vendor generated security vulnerabilities from various vendors AND the IAVAs (Information Assurance Vulnerability Alerts) from <http://www.cert.mil> that may affect the DII COE.

An entry is generated in the table below when a security vulnerability is identified. Initially, the "Course of Action" entry in the rightmost "status" field contains a URL to the security bulletin. Concurrently, a "Course of Action" report is generated and is under review by the DII COE IAVA implementation team. The COA report is not available until there is a consensus by the DII COE IAVA implementation team. This table is then updated with a Vulnerability Status Notice (VSN) report after the designated time period of review of the Course of Action report. A Patch Status Notice (PSN) report is generated after the patch has been incorporated into a DII COE segment. The PSN will contain the CM number for the media.

The bottom 3 tables are the DoD.CERT IAVAs that we track. Those originated from <http://www.cert.mil>. They have an entry also in the top (first) "vendor generated security vulnerability" table. Those 3 tables are the DoD CERT alerts, bulletins and technical advisories.

report	vulnerability	description	status
coe01-027	MS01-020.htm	Incorrect MIME Header Can Cause IE to Execute E-mail Attachment	Course of Action
coe01-026	2001 t 0003.htm	Cisco IOS Software TCP Initial Sequence Number Randomization	No COE impact
coe01-025	MS01-017.htm	Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard	*UPDATED VSN 04022001*
coe01-024	coe01-024.txt	Sec. Vulnerability in crontab(1)	Vulnerability Status Notice
coe01-023	coe01-023B.txt	w32.magistr.24876@mm aka "I-worm.Magistr" virus alert	Vulnerability Status Notice
coe01-022	MS01-016.htm	Malformed WebDAV Request Can Cause IIS to Exhaust CPU Resources	Vulnerability Status Notice
coe01-021	coe01-021.txt	Sec. Vulnerability in asecure	Vulnerability Status Notice
coe01-020	MS01-015.htm	IE can Divulge Location of Cached Content	Vulnerability Status Notice
coe01-019	2001 0002.txt	W32/Naked aka "Naked Wife" virus alert	Vulnerability Status Notice

Document: Done

Top
of page



2001 Vulnerabilities (cont.)

2001 DII COE IAVA Implementation - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Guide Print Security Shop Stop

Bookmarks Netsite: <https://disa-ca.dtic.mil/coejava/diicoejava01.htm>

This table contains the IAVAs (Information Assurance Vulnerability Alerts) from <http://www.cert.mil> that may affect the DII COE.

<i>2001 Information Assurance Vulnerability Alerts</i>			
report	vulnerability	description	status
coe01-007	2001-A-0001.htm	Buffer Overflows in Multiple Versions of ISC BIND	Vulnerability Status Notice

This table contains the IAVBs (Information Assurance Vulnerability Bulletins) from <http://www.cert.mil> that may affect the DII COE.

<i>2001 Information Assurance Vulnerability Bulletins</i>			
report	vulnerability	description	status

This table contains the Technical Advisories from <http://www.cert.mil> that may affect the DII COE.

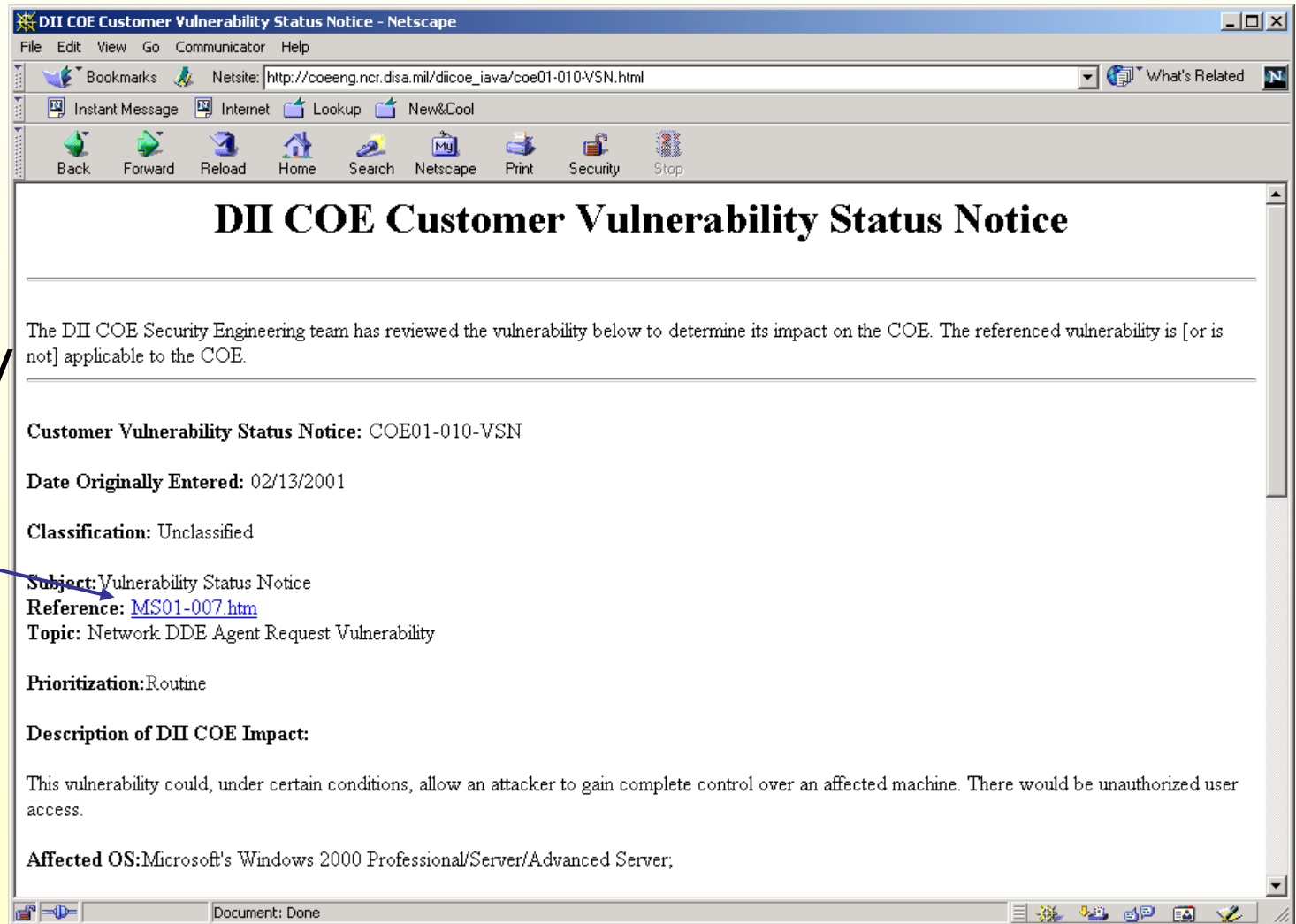
<i>2001 Technical Advisories</i>			
report	vulnerability	description	status
2001-T-0001	2001 t 0001.htm	Outlook, Outlook Express VCard Handler Contains Unchecked Buffer	*UPDATED VSN 03262001*
2001-T-0002	2001 t 0002.htm	setgid vulnerability in arp	*UPDATED VSN 03262001*
2001-T-0003	2001 t 0003.htm	Cisco IOS Software TCP Initial Sequence Number Randomization	No COE impact

Bottom
of page



Vulnerability Status Notice

Reference
to
source
vulnerability
notice



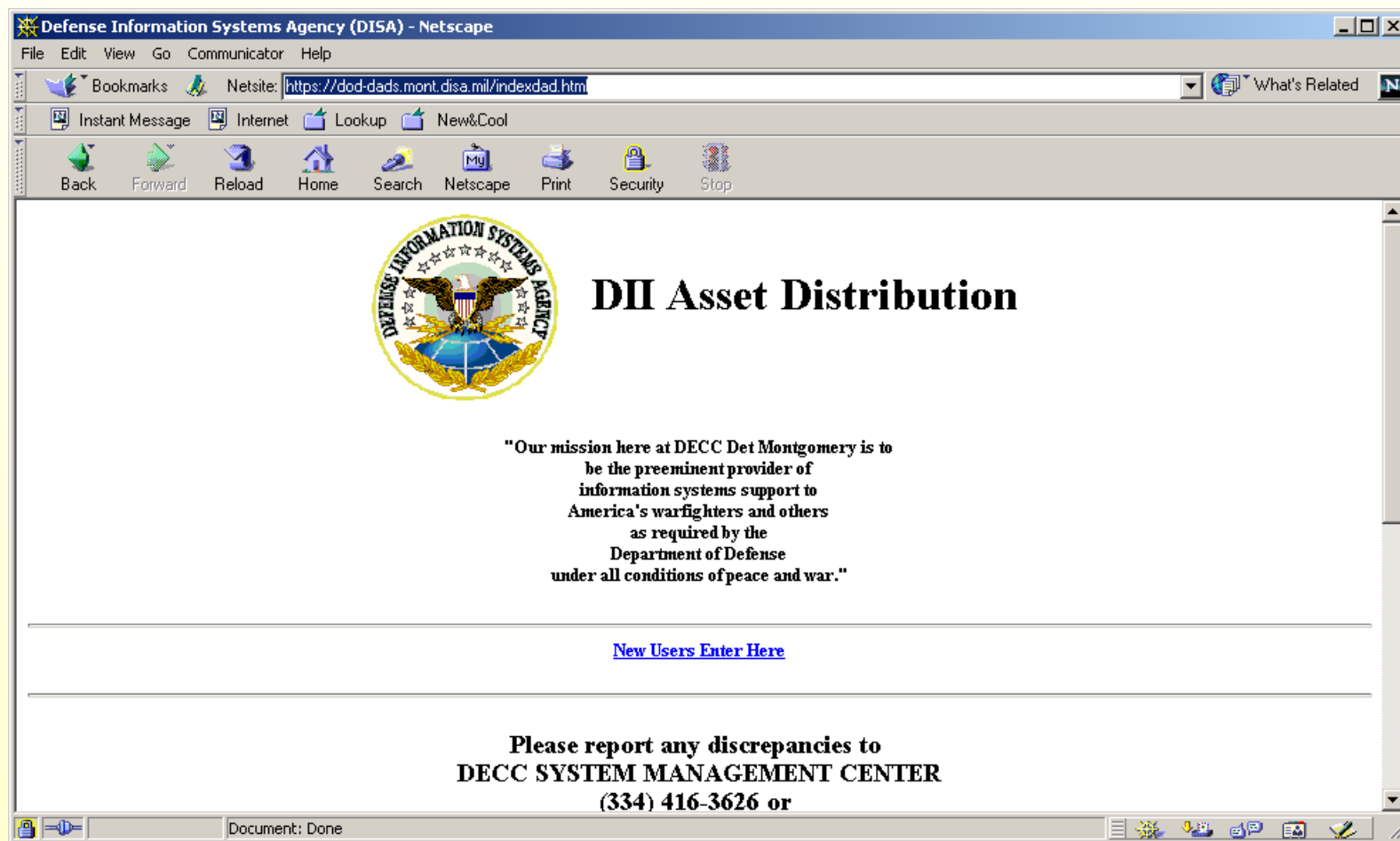


DII Asset Distribution System (DADS)

- **Internet-accessible repository for segments, patches and patch information**
- **DII COE IAVA Vulnerability Status Notices (VSNs) contain information to obtain unsegmented patch from DADS**
- **Users must first register with DADS to obtain username and password for access**



DADS Web Site





Java IAVA Issue

- **Issue:**

- **A recent IAVA identified a vulnerability in a Java Runtime Environment (JRE) included in the DII COE Java2 segments.**
- **This particular vulnerability was rated ROUTINE.**
 - **However, subsequent IAVAs may identify CRITICAL or PRIORITY vulnerabilities.**
- **A patch to fix this vulnerability will not be offered by JRE vendors**
 - **Issue arises when an application depends on a JRE with a vulnerability for which no patch exists**



Java IAVA Issue (2)

- **Assumptions:**

- **The current strategy of maintaining multiple JREs in the Java2 segments remains valid**
 - **Because JREs are not backward-compatible**
 - **Because certain COTS require specific JREs**
- **Issue is likely to occur again as vendors issue new version of software vice a patch**
 - **Need for risk management strategy to address this situation**